REMARKS

The present Amendment has pending claims 1-7.

Applicants note that the Examiner did not consider the Information Disclosure Statement submitted on May 18, 2001. A copy of the said Information Disclosure Statement is attached herewith. The Examiner is respectfully requested to consider such Information Disclosure Statement and indicate consideration thereof in the forth coming Office Action.

Claims 1-7 stand rejected under 35 USC §102(e) as being anticipated by Wiegel (U.S. Patent No. 6,484,261). This rejection is traversed for the following reasons. Applicants submit that the features of the present invention as recited in claims 1-7 are not taught or suggested by Wiegel whether taken individually or in combination with any of the other references of record. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw this rejection.

The present invention is directed to a security management, system and method for controlling or auditing a security status of each of a plurality managed systems constituting an information system in accordance with an information security policy representing a policy of security measure.

According to the present invention, a plurality of management sections are provided corresponding to at least one managed system and the information security policy wherein each management section is for controlling the security status of the managed system corresponding thereto so as to adjust the security status to the information security policy corresponding thereto, a database registering a correspondence of the information security policy, the managed system and each

management section and a security content reception section for receiving a selection of a range of the information security policy and the manage system from a user.

Further, the present invention provides an extraction section for extracting from the database the management section registered so as to correspond to the information security policy and the managed system included in the range in which the security content reception section has received the selection and a management control section for allowing the management section extracted by the extraction section to change the security status of the managed system corresponding to the management section so as to adjust to the information security policy corresponding to the management section.

Thus, according to the present invention the security status of the managed systems of an information system are controlled to implement a security policy and the security status of the managed system are audited in a manner to confirm that the managed systems are implementing the security policy.

The above described features of the present invention now more clearly recited in the claims are not taught or suggested by any of the references of record whether taken individually or in combination with each other.

Particularly, the above described features of the present invention now more clearly recited in the claims are not taught or suggested by Wiegel whether taken individually or in combination with any of the other references of record.

Wiegel teaches a graphical network security policy management method and system for managing data communication policy for network devices. Wiegel

teaches a representation of a network security policy is provided in the form of a decision tree using graphical signals wherein a user is allowed to modified properties of the graphical symbols so as to create a logical representation of the policy in other elements of the graphically displayed system.

Thus, Wiegel performs network security by the use of a guided user interface wherein graphical symbols indicating policy actions or policy conditions are assembled into a decision tree that indicates a security policy. Wiegel teaches that a script for performing the security policy indicated is generated according to the graphical symbols. The Examiner's attention is directed to col. 6, line 65 through col. 15, line 67 of Wiegel.

The present invention as recited in the claims differs substantially from that taught by Wiegel being that according to the present invention in a database a control program and/or audit program are registered according to a managed device and a security policy. Thus, according to the present invention, by executing the control program and/or the audit program corresponding to the user designated managed devices and the security policy, the designated application of the security policy and/or audit on the designated management device is performed.

The above described features of the present invention now more clearly recited in the claims are not taught or suggested by Wiegel whether taken individually or in combination with any of the other references of record.

According to the above, the system and method taught by Wiegel includes the graphical editor for designing a policy and the generator for generating the policy conformed script for setup. However, Wiegel does not teach or suggest the features

of the present invention as recited in the claims wherein security managements means and means for obtaining the status or the settings of the managing means is provided. According to the present invention, the object thereof is to simplify management procedures of the entire life cycle of a system in each phase of designing, construction and operation of the system. Such features are clearly not taught or suggested by Wiegel.

Thus, Wiegel fails to teach or suggest a plurality of management sections corresponding to the one managed system and the information security policy, wherein each management section is for controlling the security status of the management system so as to adjust the security status to the information security policy corresponding thereto and a database registering a correspondence of the information security policy, the managed system and each management section as recited in the claims.

Further, Wiegel fails to teach or suggest a security content reception section for receiving a selection of a range of the information security policy and the managed system from a user and an extraction section for extracting from the database the management section registered so as to correspond to the information security policy and the managed system included in the range in which the security content reception section has received the selection as recited in the claims.

Still further yet, Wiegel fails to teach or suggest a management control section for allowing the management section extracted by the extraction section to change the security status of the management system corresponding to the management

section so as to adjust to the information security policy corresponding to the management section as recited in the claims.

Therefore, as is quite clear from above, the features of the present invention as now more clearly recited in the claims are not taught or suggested by Wiegel whether taken individually or in combination with any of the other references of record. Accordingly, reconsideration and withdrawal of the 35 USC §102(e) rejection of claims 1-7 as being anticipated by Wiegel is respectfully requested.

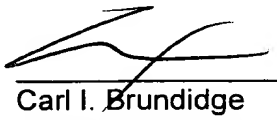
The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the reference utilized in the rejection of claims 1-7.

In view of the foregoing amendments and remarks, applicants submit that claims 1-7 are in condition for allowance. Accordingly, early allowance of claims 1-7 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER & MALUR, P.C., Deposit Account No. 50-1417 (566.39530X00).

Respectfully submitted,

MATTINGLY, STANGER & MALUR, P.C.



Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 684-1120